Thus $B(kn') < B(n')$, so n' is k-flimsy. Since $n' < 2^{2a+3} < 8k^2$, the proof is complete.

5. Some further remarks. As with all apparently irregular sequences, one can ask a large variety of questions about the distribution of sturdy and flimsy numbers. The following facts can be shown by various elementary (and sometimes simple) arguments.

For $\varepsilon > 0$ and x sufficiently large, there is a 3-flimsy number between $x - x^{2/3+\varepsilon}$ and $x + x^{2/3+\varepsilon}$; also there is a sturdy number between $x - 3x^{1/2}$ and x. There are $\gg x^{1/5}$ consecutive 3-sturdy numbers which are $\ll x$; also $\gg x^{1/5}$ consecutive 3-flimsy numbers which are $\ll x$. Given an integer $n \geqslant 1$, there is an integer $k \leqslant 2^{n-1}B(n)/n$ such that kn is sturdy, and an integer $k \leqslant 16^{(\log 2n)^2}$ such that kn is flimsy (here the logarithm is taken to the base 2).

In response to a question of the author, the referee has remarked that standard results on prime distribution in arithmetic progressions imply that at least "half" the primes are flimsy. Simply consider the primes congruent to 3 or 5 modulo 8. They satisfy

$$2^{(p-1)/2} \equiv (2/p) \equiv -1 \bmod p.$$

Hence there are integers a and k such that the relation $kp = 1 + 2^a$ holds. The referee also points out that an argument of Hasse [2] shows that in fact more than half the primes satisfy such a relation.

References

[1] E. A. Bender, *Asymptotic methods in enumeration*, SIAM Review 16 (1974), pp. 485–515.
[2] H. Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl a ≠ 0 von gerader bzw. ungerader Ordnung mod. p ist*, Math. Ann. 166 (1966), pp. 19–23.
[3] J. Muskat and K. B. Stolarsky, *The number of binary digits in multiplies of n*, in preparation.
[4] K. B. Stolarsky, *Power and exponential sums of digital sums related to binomial coefficient parity*, SIAM J. Applied Math. 32 (1977), pp. 717–730.
[5] — *The binary digits of a power*, Proc. Amer. Math. Soc. 71 (1978), pp. 1–5.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS
Urbana, Illinois 61801

Received on 23. 9. 1977
and in revised form on 23. 3. 1978 (985)

ACTA ARITHMETICA
XXXVIII (1980)

Simple groups of square order and an interesting sequence of primes

by

MORRIS NEWMAN* (Santa Barbara, Calif.), DANIEL SHANKS (College Park, Md.) and H. C. WILLIAMS (Winnipeg, Man., Canada)

1. Introduction. If a simple group has a square order, we call it a *special group*. The sequence of integers 1, 7, 41, ... given by

$$(1)\qquad s_{2m+1} = \frac{(1+\sqrt{2})^{2m+1} + (1-\sqrt{2})^{2m+1}}{2}$$

for $m = 0, 1, 2, \ldots$ we call *special numbers*. We are investigating two questions:

(A) Which finite groups are special?

(B) Which special numbers are prime?

Although Question (A) does not explicitly refer to primality, we will see that it leads us to Question (B).

A partial motivation for this investigation is the observation of R. Brauer [1] that the analysis of a simple group is facilitated if at least one prime dividing its order divides it to the first power only. Most simple groups do satisfy this Brauer condition but our special groups obviously do not.

We pursue (A) and (B) by following the closely analogous classical investigation into two much older questions:

(A_0) Which integers N are perfect?

(B_0) Which Mersenne numbers

$$(2)\qquad M_{2m+1} = 2^{2m+1} - 1$$

are prime?

As before, (A_0) does not explicitly mention primality but it leads us to (B_0) as follows:

* The work of this author was supported in part by NSF grant MCS 76-82923.

THEOREM 1_0 (Euclid). *If $M_{2m+1} = P$ is prime, then $N = P(P+1)/2$ is perfect.*

THEOREM 2_0 (Euler). *If an even $N > 6$ is perfect, then $N = P(P+1)/2$ with $P = M_{2m+1}$ prime for some m.*

THEOREM 3_0 (Cataldi). *If M_{2m+1} is prime, then $2m+1 = p$ is also prime.*

THEOREM 4_0 (Fermat, Euler). *If p is an odd prime, all positive divisors d of M_p satisfy*

$$d \equiv 1 \pmod{2p}, \qquad d \equiv \pm 1 \pmod{8}.$$

THEOREM 5_0. *If p and q are distinct odd primes, M_p and M_q are prime to each other.*

THEOREM 6_0 (Euler). *If $p \equiv 3 \pmod 4$ and $q = 2p+1$ are both prime, then q divides M_p.*

Still unsettled in this investigation are these famous questions:

(C_0) Are all perfect numbers even?

(D_0) Are infinitely many M_p prime?

(E_0) Are infinitely many M_p composite?

While Theorems 5_0 and 6_0 clearly relate to (D_0) and (E_0), respectively, they do not suffice to settle these questions.

We will see that our s_{2m+1} satisfy Theorems 3, 4, 5, and 6 which are obtained from Theorems 3_0, 4_0, 5_0, and 6_0, respectively, simply by replacing M_{2m+1} with s_{2m+1}. Analogous to Theorems 1_0 and 2_0 we now have

THEOREM 1. *If a special number s_{2m+1} is a prime P, then the symplectic group $S_p(4, P)$ is special since its order equals*

$$N = \left(P^2(P^2-1)t_{2m+1}\right)^2 \tag{3}$$

where

$$t_{2m+1} = \frac{(1+\sqrt{2})^{2m+1} - (1-\sqrt{2})^{2m+1}}{2\sqrt{2}}. \tag{4}$$

THEOREM 2. *Conversely, if a symplectic group is special, it is $S_p(4, P)$ with $P = s_{2m+1}$ prime for some m.*

Unsettled now are these open questions:

(C) Are all special groups symplectic?

(D) Are infinitely many s_p prime?

(E) Are infinitely many s_p composite?

The sequence of prime $M_p > 3$ begins with these indices:

$$p = 3, 5, 7, 13, 17, 19, 31, \tag{5}$$

while the sequence of prime s_p begins with the indices

$$p = 3, 5, 7, 19, 29, 47. \tag{6}$$

Note that M_p and s_p are both composite for $p = 11, 23, 83 \ldots$ That follows from Theorems 6_0 and 6. A necessary and sufficient condition for the primality of M_p is the well-known Lucas–Lehmer criterion. Using this, one easily extends (5) to these remaining indices $p < 1000$:

$$p = 61,\ 89,\ 107,\ 127,\ 521,\ 607. \tag{5a}$$

Unfortunately, the analogy breaks down here; we know of no useful necessary and sufficient condition for the primality of s_p. Therefore, to extend (6) to the remaining $p < 1000$ for prime s_p; namely,

$$p = 59, 163, 257, 421, 937, 947, \tag{6a}$$

requires much more elaborate methods.

We briefly discuss those methods in Section 4. Theorems 3, 4, 5, and 6 are special cases of known results of Lucas and are listed in Section 3. Theorem 2 is much more difficult. It is proven in the next section. Theorem 1 is very simple:

Proof of Theorem 1. Let $S_p(2n, q)$ be the symplectic group of dimension $2n$ over $GF(q)$. As is known, its order is

$$N = \frac{1}{d} q^{n^2} \prod_{k=1}^{n} (q^{2k}-1), \qquad d = (2, q-1). \tag{7}$$

Therefore, if $n = 2$ and q is an odd prime P, $d = 2$, and the order of $S_p(4, P)$ is

$$N = \tfrac{1}{2} P^4 (P^2-1)(P^4-1) = P^4(P^2-1)^2 \frac{P^2+1}{2}.$$

But (1) and (4) give

$$t_{2m+1}^2 = \tfrac{1}{2}(s_{2m+1}^2 + 1) \tag{8}$$

and therefore $P = s_{2m+1}$ gives (3). Since $S_p(4, P)$ is simple, the theorem follows.

Our first prime in (6) is $s_3 = 7$. This gives a well-known simple group $S_p(4, 7)$ which has $(11760)^2$ for its order. The example $S_p(4, s_{947})$ from (6a) is enormous. Since $\log_{10}(1+\sqrt{2}) = 0.382775\ldots$ we readily determine that its order is a number of 3622 digits.

2. The converse theorem. To prove the more difficult Theorem 2, we first show that the dimension $2n$ of $S_p(2n, q)$ must be 4. We generalize q to be any integer $x > 1$ and so assert

THEOREM 7. *If $x > 1$ and $d = (2, x-1)$, and if*

$$N = \frac{1}{d} x^{n^2} \prod_{k=1}^{n} (x^{2k}-1) \tag{9}$$

is a square, then $n = 2$.

We will use two well-known results:

LEMMA 1 (Bertrand's Postulate). *If n is an integer > 2, there is an odd prime p such that*

$$n/2 < p \leqslant n. \tag{10}$$

LEMMA 2. *If m and n are positive integers and x is any integer $\neq 1$, the* GCD

$$\left(\frac{x^m-1}{x-1}, \frac{x^n-1}{x-1}\right) = \frac{x^{(m,n)}-1}{x-1}. \tag{11}$$

We also use this result of Nagell [6] and Ljunggren [5]:

LEMMA 3. *If $n \geqslant 3$, the only solutions of the diophantine equation*

$$y^2 = \frac{x^n-1}{x-1} \tag{12}$$

that have $|x| > 1$ are

$$\begin{cases} n = 4, x = 7, y = \pm 20, \\ n = 5, x = 3, y = \pm 11. \end{cases} \tag{13}$$

Proof of Theorem 7. We rewrite (9) as

$$N = x^{n^2}(x^2-1)^n \frac{x^4-1}{d(x^2-1)} \cdot \frac{x^6-1}{x^2-1} \cdots \frac{x^{2n}-1}{x^2-1} \tag{14}$$

where the third factor is an integer since d divides x^2+1. First assume that n is even and > 2. Since the first two factors on the right of (14) are squares, if N is a square then so is

$$N_1 = \frac{(x^4-1)}{d(x^2-1)} \cdot \frac{(x^6-1)}{(x^2-1)} \cdots \frac{(x^{2n}-1)}{(x^2-1)}.$$

Let p be the odd prime in (10). By Lemma 2, $(x^{2p}-1)/(x^2-1)$ is prime to the other factors of N_1 and so is itself a square. But $x > 1$ and $p \geqslant 3$. Lemma 3 now shows that there is no such even $n > 2$.

Suppose n is odd and > 2. If N is a square then so is

$$N_2 = x(x^2-1)N_1. \tag{15}$$

Let $(x^{2p}-1)/(x^2-1)$ be as before. It is prime to x and if it is also prime to (x^2-1) the same argument as before shows that there is no such n. Suppose the GCD

$$g = \left(x^2-1, \frac{x^{2p}-1}{x^2-1}\right) > 1.$$

Since $x^2 \equiv 1 (\operatorname{mod} g)$ we have $(x^{2p}-1)/(x^2-1) \equiv p (\operatorname{mod} g)$. Therefore, $g = p$ and $(x^{2p}-1)/(x^2-1) = py^2$.

Put

$$u = \frac{x^p-1}{x-1}, \quad v = \frac{x^p+1}{x+1} = \frac{(-x)^p-1}{(-x)-1}$$

and we have

$$uv = py^2.$$

Since p is odd, so are u and v. Therefore

$$(x+1)v-(x-1)u = 2$$

implies that $(u, v) = 1$. We cannot have $p|u$ since v cannot be a square by Lemma 3. If $p|v$, u is a square and, in (15), x is itself a square. Therefore (13) again indicates that there is no such odd $n > 2$.

Finally, when $n = 1$, we have

$$N = (x-1)x(x+1)/d.$$

If x is even, and therefore $d = 1$, N is obviously not a square. If $x \equiv 1 \pmod 4$, $x, x-1$, and $(x+1)/2$ are pairwise relatively prime. Thus, x and $x-1$ are squares with $x > 1$. That is impossible. If $x \equiv -1 \pmod 4$, $x, x+1$, and $(x-1)/2$ are pairwise relatively prime. Now x and $x+1$ are squares with $x > 1$, which is also impossible.

Therefore, if N in (9) is a square, $n = 2$ and Theorem 7 is proven.

If the N in (7) is a square, from Theorem 7 we now have

$$N = \frac{1}{d} q^4(q^2-1)(q^4-1),$$

and

$$N_1 = \frac{1}{d}(q^2+1)$$

is also a square. Clearly, q is odd, d equals 2, and for Theorem 2 we want to show that q is not a power of a prime but a prime itself. As before, we generalize and assert

THEOREM 8. *If $m \geqslant 2$ the diophantine equation*

$$x^{2m}+1 = 2y^2 \tag{16}$$

has no solution with $|x| > 1$.

It suffices to prove this for m prime. We will treat $m = p = 2$ separately. For p odd we will need the following

LEMMA 4. *Let m and n be positive integers with $n \nmid m$. Then unique integers k and r exist such that*

$$m = 2kn \pm r, \quad k \geqslant 0,\ 0 < r < n. \tag{17}$$

This "even quotient" division algorithm, which, incidentally, is essential in the reduction of binary quadratic forms, follows from the usual division algorithm by taking $2n$ as the divisor. If the resulting positive remainder is now greater than n, increase the quotient k by 1 and reduce the remainder by $2n$.

Proof of Theorem 8. If $m = 2$ in (16), $x^4+1 = 2y^2$ implies

$$y^4 - x^4 = (y^2-1)^2$$

and the solutions of this well-known equation of Fermat are given by $x = \pm 1$, $y = \pm 1$.

Now assume $m = p$, an odd prime, and consider the GCD

$$g = \left(x^2+1, \frac{x^{2p}+1}{x^2+1}\right).$$

As before, $g = 1$ or p. If $g = 1$, from

$$\frac{x^2+1}{2}\cdot\frac{x^{2p}+1}{x^2+1} = y^2,$$

$(x^{2p}+1)/(x^2+1)$ is a square, and Lemma 3 shows that only possibilities have $|x| \leqslant 1$. Since (x^2+1, p) must equal 1 for any $p \equiv 3 \pmod 4$, that proves Theorem 8 for all such p, but for $p \equiv 1 \pmod 4$ we must continue.

Now let $g = p$ and (16) implies

$$x^2+1 = 2py_1^2, \qquad \frac{x^{2p}+1}{x^2+1} = py_2^2, \qquad y = py_1y_2. \tag{18}$$

Since x and y must both be odd, we must have

$$p \equiv 1 \pmod 8) \tag{19}$$

and, specifically, $p \geqslant 17$. For each such prime p, there is an odd q such that

$$1 < q < p, \qquad \left(\frac{q}{p}\right) = -1, \tag{20}$$

that is, q is an odd, positive, quadratic nonresidue of p that is less than p. Since $(q, p) = 1$, if we iterate the even quotient division algorithm (17),

we obtain a chain of positive integers r_i:

$$\begin{aligned}
p &= 2kq \pm r, & 0 &< r < q,\\
q &= 2k_1 r \pm r_1, & 0 &< r_1 < r,\\
r &= 2k_2 r_1 \pm r_2, & 0 &< r_2 < r_1,\\
r_1 &= 2k_3 r_2 \pm r_3, & 0 &< r_3 < r_2,\\
&\cdots\cdots\cdots\cdots & &\\
r_{s-2} &= 2k_s r_{s-1} \pm r_s, & 0 &< r_s < r_{s-1},\\
r_{s-1} &= k_{s+1} r_s & &
\end{aligned} \tag{21}$$

and must have

$$r_s = 1. \tag{22}$$

The proof now is a modification of Chao Ko's proof [4] that $x^n+1 = y^2$ has no non-trivial solutions for $n \geqslant 2$. Put

$$u = -x^2, \qquad E_n = \frac{u^n-1}{u-1} \tag{23}$$

where n is an odd, positive integer. Then $u \equiv -1 \pmod 8$, $E_n > 0$ and $E_n \equiv 1 \pmod 8$. If m and n in (17) are both odd, then so is r. If $m = 2kn + r$, we have

$$E_m = E_{2kn}u^r + E_r. \tag{24}$$

If $m = 2kn - r$, we have

$$E_{2kn} = E_m u^r + E_r. \tag{25}$$

Since $-u \equiv E_m \equiv 1 \pmod 8$, both (24) and (25) yield

$$\left(\frac{E_m}{E_n}\right) = \left(\frac{E_r}{E_n}\right) = \left(\frac{E_n}{E_r}\right), \tag{26}$$

the last equation following from the Jacobi reciprocity law.

Let us apply (26) to (18) and the first equation in (21). Then

$$p = 2kq \pm r, \qquad py_2^2 = E_p$$

gives us

$$\left(\frac{E_r}{E_q}\right) = \left(\frac{E_p}{E_q}\right) = \left(\frac{p}{E_q}\right).$$

Further, since $x^2+1 = 2py_1^2$,

$$u \equiv 1 \pmod p \qquad \text{and} \qquad E_q = \frac{u^q-1}{u-1} \equiv q \pmod p,$$

and we may continue:

$$\left(\frac{p}{E_q}\right) = \left(\frac{E_q}{p}\right) = \left(\frac{q}{p}\right) = -1.$$

Therefore, (18) leads to

$$\left(\frac{E_r}{E_q}\right) = -1. \tag{27}$$

But now apply (26) to the chain of r_i in (21). That gives

$$\left(\frac{E_r}{E_q}\right) = \left(\frac{E_q}{E_r}\right) = \left(\frac{E_{r_1}}{E_r}\right) = \left(\frac{E_r}{E_{r_1}}\right) = \ldots = \left(\frac{E_{r_s}}{E_{r_{s-1}}}\right).$$

But $r_s = 1$ and $E_{r_s} = 1$. Therefore

$$\left(\frac{E_r}{E_q}\right) = +1, \tag{28}$$

and the contradiction shows that there are no solutions of (18). That completes the proof of Theorem 8.

Now we can complete the proof of Theorem 2. With Theorems 7 and 8 we have shown that if a symplectic group has a square order it is $S_p(4, P)$ with P an odd prime that satisfies

$$P^2+1 = 2Q^2.$$

Thus

$$P^2-2Q^2 = -1,$$

and if ε is the fundamental unit of $Q(\sqrt{2})$, we therefore have

$$P+Q\sqrt{2} = \varepsilon^{2m+1} = (1+\sqrt{2})^{2m+1}$$

and $P = s_{2m+1}$. That completes the proof of Theorem 2.

3. The elementary properties of s_{2m+1}. We have

THEOREM 3. *If s_{2m+1} is a prime, then $2m+1 = p$ is also a prime.*

THEOREM 4. *If p is an odd prime, all positive divisors d of s_p satisfy*

$$d \equiv 1 \pmod{2p}, \qquad d \equiv \pm 1 \pmod{8}.$$

THEOREM 5. *If p and q are distinct odd primes, s_p and s_q are prime to each other.*

THEOREM 6. *If $p \equiv 3 \pmod 4$ is prime and $q = 2p+1$ is also prime, then q divides s_p.*

Since $s_p^2 = 2t_p^2-1$, any prime divisor of s_p must have 2 as a quadratic residue and therefore must be of the form $8k\pm 1$. Everything else in these

four theorems is merely a reflection of Lucas's laws of apparition and repetition (see, for example, Carmichael [3]) as applied to the particular Lucas functions generated by

$$x^2-2x-1 = 0.$$

The roots of this quadratic are units in $Q(\sqrt{2})$ and lead to s_{2m+1} and t_{2m+1}. We have already seen how $Q(\sqrt{2})$ enters into Theorems 1 and 2.

4. The primality of s_p. To determine which $P = s_p$ are prime we first use Fermat's theorem (for the base 13):

$$13^{P-1} \equiv 1 \pmod P. \tag{29}$$

Any P failing (29) is composite, and that eliminates all p in $50 < p < 1000$ except those listed in (6a). The six $P = s_p$ from (6a) are now "13-pseudoprimes" and are therefore very likely primes. But to prove them prime requires considerable computation since, as we mentioned above, we now have no analogue of the Lucas–Lehmer test that is so efficient for the M_p.

As an example, consider $P = s_{937}$, a number of 359 decimal digits. We will prove P prime by using the Combined Theorem of [2]. We give the exact criterion presently, but in brief this states that if we have factored $P-1$ and $P+1$ to a sufficient extent, and if their remaining unfactored factors have no prime divisors $<$ a sufficiently large bound B and if all factors obtained pass certain specific auxiliary tests, then P is prime. Now, for a 359 digit prime P chosen at random (and there must be at least 3 such P by Lemma 1), this is an impossible prescription since it is generally not feasible to "sufficiently factor" $P\pm 1$ for numbers that large.

But our s_{2m+1} are the binomials given by (1) and they have many algebraic factors. Specifically,

$$s_{2m+1}+(-1)^m = 2s_m s_{m+1},$$

$$s_{2m+1}-(-1)^m = 4t_m t_{m+1},$$

$$s_{4m+2} = (2t_{2m+1}-1)(2t_{2m+1}+1),$$

$$t_{2m} = 2s_m t_m.$$

Further, $t_m | t_n$ if $m|n$ and $s_m | s_n$ if $m|n$ and if n/m is odd. Therefore, for the $P = s_{937}$ above we have

$$\begin{aligned} P+1 &= 2s_{469}s_{468}, \\ P-1 &= 16t_{469}(2t_{117}-1)(2t_{117}+1)t_{117}s_{117}. \end{aligned} \tag{30}$$

By trial division with all primes $< B = 5\cdot 10^6$ into the several factors of (30), we obtain, first, the complete factorizations of

$$t_{117} = 5\cdot 197\cdot 389\cdot 33461\cdot 4605197\cdot P_1,$$
$$s_{117} = 7\cdot 79\cdot 199\cdot 313\cdot 599\cdot 4447\cdot 51481\cdot 4088137\cdot P_2,$$
$$2t_{117}-1 = 3^3\cdot 73\cdot 467\cdot 937\cdot 1091\cdot 4211\cdot 22307\cdot 2736707\cdot P_3.$$

Here, the large factors

$$P_1 = 36478521704768205001827888 01,$$
$$P_2 = 157737980448735483 43, \quad P_3 = 17808101758882 59049$$

are themselves proven prime by first passing (29) and then with the use of the Combined Theorem. For numbers that size the latter is both feasible and efficient. Note that some of the small factors above are algebraic. Since $117 = 9\cdot 13$, $s_9 = 7\cdot 199$, $s_{13} = 79\cdot 599$, $t_9 = 5\cdot 197$, and $t_{13} = 33461$ all appear as factors.

For the remaining factors in (30) we obtain

$$s_{469} = 239\cdot 438047\cdot H_1,$$
$$s_{468} = 17\cdot 1009\cdot 1153\cdot 1249\cdot 1873\cdot 1523089\cdot P_4\cdot H_2,$$
$$t_{469} = 13^2\cdot 4289\cdot H_3,$$
$$2t_{117}+1 = 11\cdot 179\cdot 66923\cdot H_4,$$

where $P_4 = s_{52}/s_4 = 2359699608747761281$ was proven prime as before, while the large

$$H_1 \approx 1.59\cdot 10^{171}, \quad H_2 \approx 4.14\cdot 10^{140},$$
$$H_3 \approx 1.62\cdot 10^{173}, \quad H_4 \approx 3.27\cdot 10^{36}$$

remain unfactored.

So we have

$$P-1 = F_1 H_3 H_4, \quad P+1 = F_2 H_1 H_2, \tag{31}$$

where $F_1 > 4.31\cdot 10^{140}$ and $F_2 > 3.48\cdot 10^{46}$ are completely factored and where the H_i have no prime factors less than $B = 5\cdot 10^6$. Therefore,

$$P < 2.29\cdot 10^{358} < 4.05\cdot 10^{363} < \tfrac{1}{2}F_1^2 F_2 B^3. \tag{32}$$

By a criterion in the Combined Theorem, P is thus proven prime since the factors found also pass the required auxiliary tests.

The observant reader will notice that we were lucky with s_{937}. As B is increased from $4\cdot 10^6$ to $5\cdot 10^6$ we pick up 4605197 and 4088137 as factors of t_{117} and s_{117} and thereby also find the large prime factors P_1 and P_2. Absent these, the product $\frac{1}{2}F_1^2 F_2 B^3$ on the right of (32) would be much too small to satisfy that criterion. With s_{947} we were not that lucky and much more computation was needed. The fact that the "unfactored"

$$H_3 H_4 \quad \text{and} \quad H_1 H_2$$

nonetheless are here factored algebraically into two factors was not used above. It could be used, with a slightly more complicated criterion.

Other sequences generated by binomial exponentials similar to (1) can obviously be treated similarly to our treatment of s_p above. One such is the famous Fibonacci sequence, and John Brillhart has, in fact, proven some large Fibonacci numbers prime by similar methods.

5. Going beyond. In the introduction, we asked: "(C) Are all special groups symplectic?" We have not found a single special group aside from those given by Theorem 1. However, we have not systematically examined all other known simple groups and proved that none is special. Even if we had done so, it would remain pointless to conjecture that the answer to (C) is "yes" since there would remain all of the sporadic simple groups yet to be discovered.

If the announced program of D. Gorenstein (see the New York Times, May 17, 1977) to characterize and generate all simple groups is successful, it may then be possible to settle question (C). If so, that would be another break in our analogy since we see no prospect at all that question (C_0) (about perfect numbers) will be settled in the near future.

In contrast, the heuristic arguments for questions (D) and (E) are quite convincing and we do conjecture:

(D′) There are infinitely many prime s_p and therefore infinitely many special groups.

(E′) There are infinitely many composite s_p.

We also applied the 13-pseudoprime test (29) to all $P = s_p$ in the range $1000 < p < 2000$ and found that

$$s_{1493} \quad \text{and} \quad s_{1901} \tag{33}$$

alone pass the test. They are almost certainly primes but we have not proven them to be primes.

We must leave (33) as a challenge problem: Devise a more efficient primality test for s_p than that given above and prove that s_{1493} and s_{1901} are primes.

References

[1] R. Brauer, *On groups whose order contains a prime number to the first power, I, II*, Amer. J. Math. 64 (1942), pp. 401–440.

[2] John Brillhart, D. H. Lehmer and J. L. Selfridge, *New primality criteria and factorizations of $2^m \pm 1$*, Math. Comp. 29 (1975), pp. 620–647.

[3] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math. 15 (1913–1914), pp. 30–70.

[4] Chao Ko, *On the diophantine equation* $x^2 = y^n + 1$, $xy \neq 0$, Scientia Sinica (Notes), 14 (1964), pp. 457–460.

[5] W. Ljunggren, *Some theorems on indeterminate equations of the form* $\frac{x^n - 1}{x - 1} = y^q$, Norsk Mat. Tidsskr. 25 (1943), pp. 17–20.

[6] T. Nagell, *Sur l'impossibilité de l'equation indéterminée* $z^p + 1 = y^2$, Norsk Mat. Forenings Skrifter 1 (1921), Nr. 3.

INSTITUTE FOR THE INTERDISCIPLINARY APPLICATIONS OF ALGEBRA AND COMBINATORICS and MATHEMATICS DEPARTMENT
UNIVERSITY OF CALIFORNIA SANTA BARBARA
Santa Barbara CA 93106

MATHEMATICS DEPARTMENT
UNIVERSITY OF MARYLAND
College Park, Maryland 20742

COMPUTER SCIENCE DEPARTMENT
UNIVERSITY OF MANITOBA
Winnipeg, Manitoba R3T 2N2, Canada

Received on 12. 11. 1977 (1000)

ACTA ARITHMETICA
XXXVIII (1980)

On Waring's problem

by

K. Thanigasalam (Monaca, Pa.)

1. Introduction. Among the various estimates known for $G(k)$ in Waring's problem, the most significant (for large k) are the following:

$$G(k) < k(2\log k + 4\log\log k + 2\log\log\log k + 13) \quad \text{for} \quad k \geqslant 170000 \tag{1}$$

and

$$G(k) \leqslant k(3\log k + 5.2) \quad \text{for} \quad k \geqslant 15. \tag{2}$$

These are due to Vinogradov [12] and Chen [1] respectively. Although (1) is better than (2) for sufficiently large k, for a large number of values of k, (2) is a better estimate than (1).

In this paper, we improve on (2) and prove the following:

Theorem 1. $G(k) \leqslant k(3\log k + \log 108) < k(3\log k + 4.7)$. (The improvement being by essentially $k/2$.)

For special (small) values of k Theorem 1 can be improved by modifying the method. For $k \leqslant 10$, H. Davenport [3], [4] and V. Narasimhamurti [10] obtained improvements on the estimates given by T. Estermann [7]. R. J. Cook [2] later showed that

$$G(9) \leqslant 96 \quad \text{and} \quad G(10) \leqslant 121. \tag{3}$$

Theorem 2 is an improvement on (3). The paper of R. C. Vaughan [11] containing the following results appeared since the results of this paper were obtained. A brief comparison of the methods is made towards the end of the paper.

$$G(9) \leqslant 91,\quad G(10) \leqslant 107,\quad G(11) \leqslant 122,\quad G(12) \leqslant 137,\quad G(13) \leqslant 153,$$
$$G(14) \leqslant 168,\quad G(15) \leqslant 184,\quad G(16) \leqslant 200,\quad G(17) \leqslant 216. \tag{4}$$

In this paper, we prove the following:

Theorem 2. $G(9) \leqslant 90$, $G(10) \leqslant 106$.